



Department of Defense

DIRECTIVE
AD-A272 551



February 20, 1991
NUMBER 5205.8

ASD(C3I)

SUBJECT: Access to Classified Cryptographic Information

- References:
- (a) National Telecommunications and Information Systems Security Policy (NTISSP) No. 3, "National Policy for Granting Access to U.S. Classified Cryptographic Information," December 19, 1988
 - (b) Executive Order 12333, "United States Intelligence Activities," December 4, 1981
 - (c) National Telecommunications and Information Systems Security Instruction (NTISSI) No. 4001, "Controlled Cryptographic Items," March 25, 1985
 - (d) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982
 - (e) through (i), see enclosure 1

A. PURPOSE

This Directive establishes under reference (a) a program to govern the granting of access to classified cryptographic information that is owned, produced by or for, or is under the control of the Department of Defense and is in accordance with reference (b) to protect national security information.

B. APPLICABILITY AND SCOPE

This Directive:

1. Applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Unified and Specified Commands, the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

2. Applies to all members of the U.S. Armed Forces, civilian employees of the Department of Defense and employees of agents of the DoD Components who have access to classified cryptographic information. The term "agents," as used herein, refers to contractors, consultants, and other persons affiliated with the Department of Defense.

93-26888



2px

3. Pertains to persons whose duties require continuing access to classified cryptographic information. (See section C., below.) Accordingly, this Directive concerns those persons assigned:

a. As cryptographic material custodians, alternates, or their equivalents.

b. As producers or developers of cryptographic key or logic.

c. As cryptographic maintenance, engineering, or installation technicians.

d. To supply points where cryptographic keying materials are generated or stored, and to those having access to such materials.

e. To secure telecommunications facilities located on the ground, on board ship, or on communications support aircraft and whose duties require keying of cryptographic equipment.

f. To prepare, authenticate, or decode nuclear control orders (valid or exercise).

g. Any responsibility requiring or enabling access to classified cryptographic media.

4. Is not applicable to individuals whose duties are to operate (not to key or maintain) systems using cryptographic equipment.

5. Excludes Controlled Cryptographic Items as defined in NTISSI No. 4001 (reference (c)).

C. DEFINITION

Classified Cryptographic Information, with respect to this access program, is specified as:

1. Cryptographic key and authenticators that are classified pursuant to DoD 5200.1-R (reference (d)) and are designated as SECRET CRYPTO, or TOP-SECRET CRYPTO.

2. Classified cryptographic media that embody, describe, or implement a classified cryptographic logic, to include, but not be limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic computer software.

D. POLICY

It is DoD policy that a person may be granted access to classified cryptographic information, as specified in sections B. and C., above, only if that person:

1. Is a U.S. citizen;
2. Is a civilian employee of the Department of Defense, a member of a Military Service, a DoD-cleared contractor or employee of such contractor, or is employed as a DoD representative (including consultants of the Department of Defense);
3. Requires access to perform official duties for, or on behalf of, the Department of Defense;
4. Possesses a security clearance and personnel security investigation appropriate to the level of the classified cryptographic information to be accessed, in accordance with DoD 5200.2-R (reference (e));
5. Receives a security briefing appropriate to the cryptographic information to be accessed;
6. Acknowledges the granting of access by signing a cryptographic access certificate;
7. Agrees to report foreign travel and any form of contact with foreign citizens, in accordance with DoD 5200.2-R (reference (e)); and
8. Acknowledges the possibility of being subject to a non-lifestyle, counterintelligence scope polygraph examination administered in accordance with DoD Directive 5210.48 (reference (f)).

E. RESPONSIBILITIES

1. The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence shall oversee and review the implementation of this Directive.
2. The Heads of the DoD Components shall:
 - a. Control access to classified cryptographic information in accordance with section D., above.

b. Establish, implement, and administer a cryptographic access program within their respective organizations. This program shall include providing Cryptographic Access Briefings (sample in enclosure 2) and executing Cryptographic Access Certificates (sample in enclosure 3).

c. Implement, in accordance with DoD Directive 5210.48 (reference (f)), a counterintelligence scope polygraph examination program in support of this Directive.

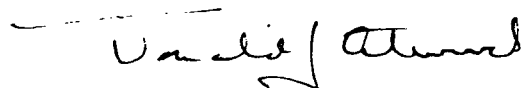
d. Maintain records on all individuals who have been granted cryptographic access or have had their cryptographic access withdrawn, and arrange for retention of Cryptographic Access Certificates or legally enforceable facsimiles in accordance with the DoD Component records disposition schedules.

e. Accept as valid the cryptographic access granted by other DoD Components.

f. Deny or withdraw cryptographic access to those individuals who fail to agree to or comply with the specific criteria identified in section D., above.

F. EFFECTIVE DATE

This Directive is effective immediately.



Donald J. Atwood
Deputy Secretary of Defense

Enclosures - 3

1. References
2. Sample - Cryptographic Access Briefing
3. SD Form 572 - Cryptographic Access Certification and Termination

Feb 20, 91
5205.8 (Encl 1)

REFERENCES, continued

- (e) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, December 20, 1979
- (f) DoD Directive 5210.48, "DoD Polygraph Program," December 24, 1984
- (g) DoD Directive 5220.22, "DoD Industrial Security Program," December 8, 1980
- (h) DoD 5220.22-R, "Industrial Security Regulation," December 1985, authorized by DoD Directive 5220.22, December 8, 1980
- (i) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," March 1989, authorized by DoD Directive 5220.22, December 8, 1980

Accession For	
NTIS	DTIC
DTIC	DTIC
per form 50	
By	
DT	
Date	
A-1	

DTIC QUALITY INSPECTED 8

SAMPLE

CRYPTOGRAPHIC ACCESS BRIEFING

You have been selected to perform duties that will require access to classified cryptographic information. It is essential that you be made aware of certain facts relevant to the protection of this information before access is granted. You must know the reason why special safeguards are required to protect classified cryptographic information. You must understand the Directives that require these safeguards and the penalties you may incur for the unauthorized disclosure, unauthorized retention, or negligent handling of classified cryptographic information. Failure to properly safeguard this information could cause serious or exceptionally grave damage, or irreparable injury, to the national security of the United States or could be used to advantage by a foreign nation.

Classified cryptographic information is especially sensitive because it is used to protect other classified information. Any particular piece of cryptographic keying material and any specific cryptographic technique may be used to protect a large quantity of classified information during transmission. If the integrity of the cryptographic system is breached at any point, all information protected by the system may be compromised. The safeguards placed on classified cryptographic information are a necessary component of Government programs to ensure that our nation's vital secrets are not compromised.

Because access to classified cryptographic information is granted on a strict need-to-know basis, you will be given access to only that cryptographic information necessary in the performance of your duties. You are required to become familiar with (insert, as appropriate, Department or Agency implementing Directives covering the protection of cryptographic information). Cited Directives are attached in a briefing book for your review at this time.

Especially important to the protection of classified cryptographic information is the timely reporting of any known or suspected compromise of this information. If a cryptographic system is compromised, but the compromise is not reported, the continued use of the system can result in the loss of all information protected by it. If the compromise is reported, steps can be taken to lessen an adversary's advantage gained through the compromise of the information.

As a condition of access to classified cryptographic information, you must acknowledge that you may be subject to a non-life-style, counterintelligence scope polygraph examination. This examination will be administered in accordance with DoD Directive 5210.48

and applicable law. The relevant questions in this polygraph examination will only encompass questions concerning espionage, sabotage, or questions relating to unauthorized disclosure of classified information or unreported foreign contacts. If you do not, at this time, wish to sign such an acknowledgment as a part of executing a cryptographic access certification, this briefing will be terminated at this point and the briefing administrator will so annotate the cryptographic access certificate. Such refusal will not be cause for adverse action but will result in your being denied access to classified cryptographic information.

You should know that intelligence services of some foreign governments prize the acquisition of classified cryptographic information. They will go to extreme lengths to compromise U.S. citizens and force them to divulge cryptographic techniques and materials that protect the nation's secrets around the world. You must understand that any personal or financial relationship with a foreign government's representative could make you vulnerable to attempts at coercion to divulge classified cryptographic information. You should be alert to recognize those attempts so that you may successfully counter them. The best personal policy is to avoid discussions that reveal your knowledge of, or access to, classified cryptographic information and thus avoid highlighting yourself to those who would seek the information you possess. Any attempt, either through friendship or coercion, to solicit your knowledge regarding classified cryptographic information must be reported immediately to (insert appropriate security office).

In view of the risks noted above, unofficial travel to certain communist or other designated countries may require the prior approval of (insert appropriate security office). It is essential that you contact (insert appropriate security office) if such unofficial travel becomes necessary.

Finally, you must know that, should you willfully or negligently disclose to any unauthorized persons any of the classified cryptographic information to which you will have access, you may be subject to administrative and civil sanctions, including adverse personnel actions, as well as criminal sanctions under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate.

CRYPTOGRAPHIC ACCESS CERTIFICATION AND TERMINATION**Privacy Act Statement**

AUTHORITY: EO 9397, EO 12333, and EO 12356.
PRINCIPAL PURPOSE(S): To identify the individual when necessary to certify access to classified cryptographic information.
ROUTINE USE(S): None.
DISCLOSURE: Voluntary; however, failure to provide complete information may delay certification and, in some cases, prevent original access to classified cryptographic information.

INSTRUCTIONS

Section I of this certification must be executed before an individual may be granted access to classified cryptographic information.
 Section II will be executed when the individual no longer requires such access.

Until cryptographic access is terminated and Section II is completed, the cryptographic access granting official shall maintain the certificate in a legal file system, which will permit expeditious retrieval. Further retention of the certificate will be as specified by the DoD Component record schedules.

SECTION I - AUTHORIZATION FOR ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

- a. I understand that I am being granted access to classified cryptographic information. I understand that my being granted access to this information involves me in a position of special trust and confidence concerning matters of national security. I hereby acknowledge that I have been briefed concerning my obligations with respect to such access.
- b. I understand that safeguarding classified cryptographic information is of the utmost importance and that the loss or compromise of such information could cause serious or exceptionally grave damage to the national security of the United States. I understand that I am obligated to protect classified cryptographic information and I have been instructed in the special nature of this information and the reasons for the protection of such information. I agree to comply with any special instructions, issued by my department or agency, regarding unofficial foreign travel or contacts with foreign nationals.
- c. I acknowledge that I may be subject to a non-lifestyle, counterintelligence scope polygraph examination to be administered in accordance with DoD Directive 5210.48 and applicable law.
- d. I understand fully the information presented during the briefing I have received. I have read this certificate and my questions, if any, have been satisfactorily answered. I acknowledge that the briefing officer has made available to me the provisions of Title 18, United States Code, Sections 641, 793, 794, 798, and 952. I understand that, if I willfully disclose to any unauthorized person any of the U.S. classified cryptographic information to which I might have access, I may be subject to prosecution under the Uniform Code of Military Justice (UCMJ) and/or the criminal laws of the United States, as appropriate. I understand and accept that unless I am released in writing by an authorized representative of (insert appropriate security office) _____, the terms of this certificate and my obligation to protect all classified cryptographic information to which I may have access, apply during the time of my access and at all times thereafter.

ACCESS GRANTED THIS _____ DAY OF _____, 19 ____.

1. EMPLOYEE

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE / RANK / RATING	d. SOCIAL SECURITY NO.
--------------	---------------------------------------	--------------------------	------------------------

2. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION
--------------	---------------------------------------	----------	----------------------

SECTION II - TERMINATION OF ACCESS TO CLASSIFIED CRYPTOGRAPHIC INFORMATION

I am aware that my authorization for access to classified cryptographic information is being withdrawn. I fully appreciate and understand that the preservation of the security of this information is of vital importance to the welfare and defense of the United States. I certify that I will never divulge any classified cryptographic information I acquired, nor discuss with any person any of the classified cryptographic information to which I have had access, unless and until freed from this obligation by unmistakable notice from proper authority. I have read this agreement carefully and my questions, if any, have been answered to my satisfaction. I acknowledge that the briefing officer has made available to me Title 18, United States Code, Sections 641, 793, 794, 798, and 952; and Title 50, United States Code, Section 783(b).

ACCESS WITHDRAWN THIS _____ DAY OF _____, 19 ____.

3. EMPLOYEE

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE / RANK / RATING	d. SOCIAL SECURITY NO.
--------------	---------------------------------------	--------------------------	------------------------

4. ADMINISTERING OFFICIAL

a. SIGNATURE	b. NAME (Last, First, Middle Initial)	c. GRADE	d. OFFICIAL POSITION
--------------	---------------------------------------	----------	----------------------